УДК 004.056.5

ENTERPRISE INFORMATION SECURITY

Шевцов Н.П.,
Научный руководитель преподаватель Юрданова В.Н.
Сибирский федеральный университет

If you spend more on coffee than on IT security, you will be hacked.
What's more, you deserve to be hacked.
—White House Cybersecurity Advisor, Richard A. Clarke (b. 1950)

Recently, Information Security has received a lot of attention in the business and trade press in the Russian Federation and in general around the world.
Much of this can be attributed to an increase in security breaches leading to major losses to affected enterprises. More and more companies are implementing a formal enterprise security architecture process to support the governance and management of IT.

There are many different attack types ranging from web-site defacement to financial fraud to Internet worms and viruses (e.g. Trojans, rootkits, etc.), so that I can recognize attacks by their atypical effects. There are several reports of the world-famous expers in the field of Information Security that point to the increasing number of vulnerabilities in commonly used software as well as viruses and other threats that seek to exploit these vulnerabilities, and detail, how it is becoming an increasing problem for enterprises. Effective countermeasures sometimes exist for many of these threats, but are often not correctly deployed due to the specific characteristics of the information systems in use, or the capabilities of the IT staff.

The economic analysis of information security has many dimensions to it as evidenced by the literature including risk management approaches, insurance, vulnerability analysis (e.g. [1][1]), information sharing, etc. However, the role of decision making within the enterprise and the related issues of incentives and information assymetry within a firm has not received much attention in the context of information security. Therefore, the making of optimal information security deployment desicions in the light of the above factors is an integral part of Enterprise Information Security (EIS).

I have been focused much attention on detailing the operation of countermeasures (e.g. firewalls that protect against unauthorized traffic) but little attention is focused on who in the enterprise is making decisions regarding deployment of these measures and what policies are in place to deal with such decision making.
When diskussing Enterprise Information Security, it is important to understand that enterprises are not homogeneous entities and their divisions often use varied information systems, which are commonly interconnected with each other as well as to the Internet (e.g. via insecure network, when it has a risk to be damaged, distructured or may be readed by eavesdroppers or hackers by means of packet sniffing).

The key goal of my paper is to explore some basic theoretical and methodological aspects and principles of Enterprise Information Security such as:

- Minimum Enterprise Information Security Standards and Rules
- Different kinds of countermeasures (e.g. Physical Security)

---

[1] D. Wagner and D. Dean. *Instrusion Detection via Static Analysis* of *IEEE Symposium on Security and Privacy.*, 2001.

- Differential Privacy
- Confidentiality, Integrity and Availability

I try to model the strategic steps of management of the enterprise maintaining security of information. My paper is inspired by Vitaly Shmatikov et al [2][2] and Cynthia Dwork's work [3][3] which both look at these problems in Information Security context, albeit with a different application in mind. This paper will discuss an approach to Enterprise Information Security Rights. It will describe an enterprise security policy, security domains, trust levels, secure local and wide area networks, and most importantly the relationships among them.

As stated, "Most companies do not adopt published security management standards, but choose to write their own. This means that consistent, effective security standards are unlikely to be applied across different organizations." (Information Security Forum, p.1).
There is not a one-size-fits-all policy that will suit the needs of all corporations. However, by accepting a recommended approach to enterprise security architecture, corporate security programs may become more consistent and effective. Information technology has transformed traditional business models and facilitated the creation of entirely new ones by integrating technology into business processes. With this integration, the lines between Information Security and traditional Physical Security have become blurred because as with business processes that rely on technology, so too, Information Security and Physical Security have become inextricably linked.

This work opens up many avenues for future research. I expect that I could achieve deep understanding by further research and offer new technological methods. I relied on a strategic combination of Physical Security as a critical component of Computer Security and Information Security. This combination yields better results that either method alone and presents a promising new approach to the Enterprise Information Security problem.

[2] J. Brickell, V. Shmatikov. The Cost of Privacy: Destruction of Data-Mining Utility in Anonymized Data Publishing. *KDD.*, 2008.

[3] S. Dwork. A Firm Foundation for Private Data Analysis. *ACM.*, 2011.